# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PLAN DE ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD

El Pleno de la Corporación, en sesión ordinaria celebrada el día 17 de enero de 2014, adoptó, entre otros, el siguiente acuerdo:

"Aprobar la Política de Seguridad de la Información, así como el Plan de Adecuación de la Diputación Provincial de Huesca, para adaptarse a las previsiones contenidas en el Esquema Nacional de Seguridad, regulado por el Real Decreto 3/2010, de 8 de enero, conforme a los términos obrantes en el expediente, dando publicidad a los mencionados documentos en el Boletín Oficial de la Provincia, así como en la sede electrónica de esta Diputación".

**Texto íntegro Política Seguridad de la Información:**

## "1.- APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 17 de enero de 2014 por el Pleno de la Diputación Provincial de Huesca.

Esta "Política de Seguridad de la Información", en adelante Política, es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

## 2.- INTRODUCCIÓN

El desarrollo de la Administración Electrónica implica el tratamiento de gran cantidad de información por parte de los sistemas de tecnologías de la información y de las comunicaciones. La información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. El Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiaran la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Al objeto de dar cumplimiento al ENS, la Diputación Provincial de Huesca, conocedora de los riesgos que pueden afectar a los sistemas de información, que soportan los trámites electrónicos puestos a disposición a la ciudadanía, y teniendo en cuenta que ésta pone a su disposición su activo más valioso "su propia Información" es consciente de que éstos deben ser administrados con la suficiente diligencia, y que se deben de tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

De este modo, todos los departamentos y/o áreas de la Diputación Provincial de Huesca, que se encuentran dentro del ámbito del ENS, tienen presente que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, para la Diputación Provincial de Huesca, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los

servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el Artículo 7 del ENS.

### 2.1 Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Diputación Provincial de Huesca implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la Diputación Provincial de Huesca:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

### 2.2 Detección

La Diputación Provincial de Huesca establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS (reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 8 del ENS. Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

### 2.3 Respuesta

La Diputación Provincial de Huesca establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

### 2.4 Recuperación

Para garantizar la disponibilidad de los servicios, la Diputación Provincial de Huesca dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

## 3.- MISIÓN DE LA DIPUTACIÓN PROVINCIAL DE HUESCA

La Diputación Provincial de Huesca pone a disposición de la ciudadanía la realización de trámites online con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la eficacia de la acción pública.

Potenciando por otro lado también, el uso de las nuevas tecnologías en la Diputación y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con la Diputación, reduciendo así los tiempos de espera y de resolución de trámites solicitados por éstos.

## 4.- ALCANCE

Esta Política se aplicará a los sistemas de información de la Diputación Provincial de Huesca, que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

Todos los miembros de la Diputación Provincial de Huesca, afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta "Política de Seguridad de la Información" y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

## 5.- MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades de la Diputación Provincial de Huesca, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía, está integrado por las siguientes normas:

a) Real Decreto 3/2010 Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
b) Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
c) Ley Orgánica 15/99 de 13 de Diciembre de Protección de Datos de Carácter Personal.
d) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
e) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
f) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
g) Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
h) Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.
i) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
j) Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.
k) Ley 59/2003, de 19 de diciembre, de firma electrónica.
l) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
m) Boletín Oficial de la Provincia de Huesca número 13 de 20 de enero de 2011, por la que se aprueba el Reglamento de Administración Electrónica de la Diputación Provincial de Huesca y del Instituto de Estudios Altoaragoneses.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Diputación Provincial de Huesca derivadas de las anteriores y publicadas en las sedes electrónica comprendidas dentro del ámbito de aplicación de de la presente Política.

## 6.- ORGANIZACIÓN DE LA SEGURIDAD

### 6.1 Estructura organizativa

La estructura organizativa de la Organización de la Seguridad de la Información en la Diputación Provincial de Huesca se estructura del siguiente modo:

### 6.2 Comité de Seguridad

El Comité estará compuesto por los siguientes:

- **Presidente:** El Diputado Presidente de la Comisión de Régimen Interior y Bienestar Social, actuando como suplente el Diputado Presidente de la Comisión de Innovación Local y Tecnología.
- Miembros:
    - **Responsable de Seguridad LOPD Técnico, que será a su vez el Responsable de Seguridad ENS:** El Jefe de los servicios informáticos, actuando como suplente el Técnico Responsable de Telecomunicaciones y Sistemas.
    - **Responsable de Seguridad LOPD Jurídico:** El Secretario General, actuando como suplente, la Jefe de Servicio de Secretaría.
- **Secretario:** Técnico de Gestión de Régimen Interior, actuando como suplente el Jefe de Negociado de Acuerdos y Resoluciones.

## 7.- RESPONSABILIDADES ASOCIADAS AL ESQUEMA NACIONAL DE SEGURIDAD

A continuación de detallan y se establecen las funciones y responsabilidades de cada una de las figuras, responsabilidades que recoge el Comité de Seguridad.

- El Responsable del Servicio, determina los requisitos de seguridad de los servicios prestados dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad ENS.
- El Responsable de la Información, determina los requisitos de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad ENS.
- El Responsable de Seguridad ENS, su función es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho.
- EL Responsable del Sistema, es el encargado de las operaciones del sistema.

### 7.1 Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

a) Atender las inquietudes del Diputación Provincial de Huesca y de los diferentes departamentos.
b) Informar regularmente del estado de la seguridad de la información al Diputación Provincial de Huesca.
c) Promover la mejora continua del sistema de gestión de la seguridad de la información.
d) Elaborar la estrategia de evolución de la Institución en lo que respecta a seguridad de la información.
e) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
f) Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por el Diputación Provincial de Huesca.
g) Aprobar la normativa de seguridad de la información.
h) Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
i) Monitorizar los principales riesgos residuales asumidos por la Institución y recomendar posibles actuaciones respecto de ellos.
j) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
k) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la Institución en materia de seguridad.

l) Aprobar planes de mejora de la seguridad de la información de la Institución. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
m) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
n) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
o) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Institución, elevando aquellos casos en los que no tenga suficiente autoridad para decidir. Procedimientos de designación.

La Diputación Provincial de Huesca ha procedido a realizar la constitución del comité y de las distintas responsabilidades. Todos los nombramientos se revisarán cada 2 años o cuando los puestos quedes vacantes.

## 8.- DATOS DE CARÁCTER PERSONAL

La Diputación Provincial de Huesca solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos. Estas medidas estarán recogidas en el Documento de Seguridad LOPD, que se encuentra bajo la custodia del Comité de Seguridad de la Información.

## 9.- OBLIGACIONES DEL PERSONAL

Todos los miembros del Diputación Provincial de Huesca, que se encuentran dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez cada al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Diputación Provincial de Huesca, en particular al de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

## 10.- GESTIÓN DE RIESGOS

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

1. Categorización de los sistemas.
2. Análisis de riesgos.

3. El Comité de Seguridad procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos se utiliza la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

## 11.- DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (políticas, protocolos, procedimientos, instrucciones técnicas, etc.)

Del mismo modo, esta Política de Seguridad de la Información complementa las políticas de seguridad de la Diputación Provincial de Huesca en materia de protección de datos de carácter personal.

La Normativa de Seguridad estará a disposición de todos los miembros de la Institución que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en Intranet

## 12.- TERCERAS PARTES

Cuando la Diputación Provincial de Huesca preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Diputación Provincial de Huesca utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.”

**Texto íntegro Plan de Adecuación al Esquema Nacional de Seguridad:**

## "1.- APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 17 de enero de 2014 por el Pleno de la Diputación Provincial de Huesca.

## 2.- INTRODUCCIÓN

El Esquema Nacional de Seguridad, en su Disposición Transitoria sobre Adecuación de los Sistema, establece que:

1. Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.
2. Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.
3. El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

## 3.- POLÍTICA DE SEGURIDAD

La Diputación Provincial de Huesca dispone de una Política de Seguridad aprobaba el 17 de enero de 2014. Esta Política de Seguridad ha sido desarrollada teniendo en cuenta los principios básicos y en base a los requisitos mínimos de seguridad establecidos por la normativa del ENS y conforme a lo exigido en el Anexo II del Real Decreto ENS, contemplando los requisitos exigidos en la sección [org. 1].

En el Anexo I, del presente documento, se adjunta la ***Política de Seguridad de la Información de la Diputación Provincial de Huesca***.

## 4.- VALORACIÓN DE LOS SERVICIOS JUNTO CON LA INFORMACIÓN QUE GESTIONAN

En el ***Anexo II***, del presente documento, se adjunta la ***Valoración de los Servicios y de la Información*** que éstos gestionan, según lo establecido en el Anexo I del ENS.

## 5.- DATOS DE CARÁCTER PERSONAL

La Diputación Provincial de Huesca dispondrá de un Documento de Seguridad adaptado al Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD).

## 6.- CATEGORÍA DEL SISTEMA

En el ***Anexo III***, al presente documento, se adjunta la ***Valoración y Categoría del Sistema*** según lo establecido en el Anexo I del ENS.

## 7.- ANÁLISIS DE RIESGOS

La Diputación Provincial de Huesca ha realizado un análisis de riesgos, según lo establecido en el Anexo II del Real Decreto en su sección [op.pl.1], en función de la categoría del sistema, en

este caso la Diputación Provincial de Huesca, ha determinado que la categoría de su sistema es de ***nivel MEDIO***.

En el **Anexo IV**, del presente documento, se adjunta el Informe de ***Riesgo Intrínseco y Residual.*** El análisis de riesgos ha sido realizado usando la metodología MAGERIT en su versión 2 (MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.).

## 8.- DECLARACIÓN DE APLICABILIDAD (Anexo II del Real Decreto ENS)

En el ***Anexo V***, del presente documento, se adjunta la ***Declaración de Aplicabilidad*** de las medidas de seguridad del Anexo II.

## 9.- INSUFICIENCIAS DEL SISTEMA

La Diputación Provincial de Huesca es consciente de tiene un cumplimiento parcial de gran parte de las medidas de seguridad establecidas en el anexo II del Real Decreto ENS y que esto es debido a la necesidad de implantar un *Sistema de Gestión de la Seguridad de la Información* (SGSI) de su Sistema. Esta insuficiencia se subsanará mediante las tareas previstas en el *Plan de Mejora de la Seguridad (Anexo VI)* de la Diputación Provincial de Huesca.

Por otro lado, la Diputación Provincial de Huesca, también presenta un cumplimiento parcial de las medidas de seguridad establecidas en el Real Decreto LOPD y de la normativa de protección de datos en general, desviaciones que en la actualidad se encuentran en fase de subsanación.

## 10.- PLAN DE MEJORA DE LA SEGURIDAD

En el ***Anexo VI***, del presente documento, se adjunta el ***Plan de Mejora de la Seguridad***, que contine las acciones necesarias para subsanar las insuficiencias detectadas.

## 11.- INTERCONEXIÓN DE SISTEMAS

La Diputación Provincial de Huesca, comunica a todos los terceros con los que maneja información la valoración de su sistema para que sea incluido en sus planes. En la actualidad, en el ámbito de los servicios o trámites electrónicos dentro del marco establecido en el ENS, están identificadas las interconexiones:

- Con la Red SARA al objeto del uso de la firma electrónica y autenticación por certificados digitales, así como el sellado en el tiempo. Esta conexión se realiza a través de la Dirección General de Aragón (DGA).
- Las Entidades Locales, conectan a los sistemas de la Diputación Provincial de Huesca, al objeto de recibir los servicios que la Diputación les proporciona.”

Lo que se publica para general conocimiento, en cumplimiento del indicado acuerdo Plenario.

Huesca, 17 de febrero de 2014

El Presidente,

Antonio José Cosculluela Bergua.